Claims

What is claimed is:

1. A method for maintaining confidential records of an individual comprising the steps of:

selecting, by the individual, a record server that is publicly accessible over a network;

encrypting a confidential record of the individual;

storing the encrypted confidential record on the selected record server; and

accessing the encrypted confidential record stored on the selected record server through a defined gateway system.

2. The method of claim 1 further comprising the step of distributing an access token to a predetermined agent by the individual for use in accessing the stored confidential record over the network.

3. The method of claim 2 wherein the predetermined agent is a healthcare institution.

4. The method of claim 1 wherein the confidential record is a medical record.

5. The method of claim 4 wherein the individual is a patient.

6. The method of claim 5 wherein the predetermined agent is the patient who has privileges to read, modify, and annotate the medical record.

7. The method of claim 2 further comprising the step of controlling, by the individual, privileges which the predetermined agent has for accessing the confidential record.

8. The method of claim 2 further comprising the step of associating a class of agents with a set of privileges for accessing the confidential record, wherein the predetermined agent is a member of the class.

9. The method of claim 2 wherein the access token is a private cryptographic key.

10. The method of claim 2 wherein the access token is a biometric of the predetermined individual that is measurable by a biometric hardware device.

11. The method of claim 2 wherein the access token is a smart-card.

12. The method of claim 2 further comprising the step of accessing by the predetermined agent the encrypted confidential

record on the record server from any node on the network capable of accepting the access token.

13. The method of claim 2 further comprising the step of maintaining anonymity of the individual when the predetermined agent accesses the encrypted confidential record of the individual.

14. The method of claim 2 further comprising the step of determining by the individual each portion of the confidential record that is accessible to the predetermined agent.

15. The method of claim 1 wherein the gateway system and the record server selected by the individual are the same node on the network.

16. The method of claim 1 further comprising the step of defining a schema for representing the confidential record using a markup language.

17. In a network, a system for providing access to confidential records of an individual comprising:

digital information representing a confidential record of the individual;

a publicly accessible server system connected to the network and selected by the individual for storing the confidential record; and

a gateway system, in communication with the server system, comprising software for accessing the confidential record of the individual.

18. The system of claim 17 further comprising:

an access token distributed to a predetermined agent by the individual for use by the gateway system in accessing the stored confidential record.

19. The system of claim 18 wherein the access token is a private cryptographic key.

20. The system of claim 18 wherein the access token is a biometric of the predetermined agent that is measurable by a biometric hardware device.

21. The system of claim 18 wherein the access token is a smart-card.

22. The system of claim 17 further comprising a mapper in communication with the gateway system, the mapper associating a predetermined agent with a class of agents that has privileges to access the confidential record.

23. The system of claim 22 wherein the predetermined agent is the individual who has privileges to read, write, and annotate the confidential record.

24. The system of claim 22 wherein the predetermined agent is a healthcare institution whose privileges to access the confidential record are controlled by the individual.

25. The system of claim 17 wherein the gateway system and the record server selected by the individual are the same node on the network.

26. The system of claim 17 wherein the confidential record includes a link to an electronic document that is accessible over the network.

27. The system of claim 17 wherein the confidential record is a medical record.

28. The system of claim 27 wherein the individual is a patient.

29. The system of claim 17 wherein the confidential record includes at least one record object, each record object including a privilege section associating a class of agents with a set of privileges for accessing that record object.